UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Newport News Division

APRIL DARRIN, *et al.,* individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

HUNTINGTON INGALLS INDUSTRIES,

Defendant.

Case No. 4:23-cv-53

CONSOLIDATED AMENDED COMPLAINT

[JURY TRIAL DEMANDED]

Representative Plaintiffs allege as follows:

INTRODUCTION

1. Representative Plaintiffs April Darrin, Kenneth D. Keeler, Cheryl Soles, Tyler N. Beadle and Bruce Snyder ("Representative Plaintiffs") bring this class action against Defendant Huntington Ingalls Industries ("Defendant" or "HII") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' protected health information and personally identifiable information stored within Defendant's information network, including without limitation full names, Social Security numbers, credit card numbers, debit card numbers, dates of birth, driver's license numbers, state identification numbers, tax identification numbers, personal identification numbers, military identification, passport numbers, financial account information, routing numbers, health insurance information and medical information (these types

of information, *inter alia*, being thereafter referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII"[2]).

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and, at least, 43,643[3] other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant between March and May 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII which was being kept unprotected (the "Data Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

4. While Defendant claims to have discovered the breach as early as March 2022, Defendant did not begin informing victims of the Data Breach until April 18, 2023—over a year after the Data Breach was believed to have first begun. Due to the cryptic language Defendant purposefully used in notifying victims of the Breach, it is unclear precisely when Defendant discovered the Breach.

5. Defendant's notice of breach, mailed to Plaintiffs on April 18, 2023 (the "Notice") made unclear the nature of the Breach and the threat it posed—refusing to tell its consumers how

---

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

[3] "*Data Breach Notification,"* https://apps.web.maine.gov/online/aeviewer/ME/40/ba2846ca-c8ca-4c24-94fa-6f239a70fbf8.shtml (last accessed April 27, 2023).

many people were impacted, how the breach happened, or why it took the Defendant over a year to begin notifying victims that hackers had gained access to their highly private PHI/PII.

6. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft and unable to monitor their financial accounts or credit reports to prevent unauthorized use of their PHI/PII.

7. Defendant's breach differs from typical data breaches because it affects consumers who had no relationship with Defendant, never sought a relationship with Defendant and never consented to Defendant collecting and storing their information.

8. Defendant sourced its information from third parties, stored it on its servers and assumed a duty to protect it, advertising that HII "uses reasonable organizational, technical, and administrative measures to provide a level of security appropriate to the risk associated with the Personal Information [it would] collect."[4]

9. Defendant's privacy policy states, "[HII does] not sell, transfer, or otherwise disclose Personal Information that [it collects] from or about [consumers]."[5]

10. Despite its promises and acknowledgement of the importance of cybersecurity, HII never implemented the security safeguards needed.

11. Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' PHI/PII. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiffs and Class Members would use Defendant's services, directly or indirectly, to store and/or share sensitive data, including highly confidential PHI/PII.

12. HIPAA establishes national minimum standards for the protection of individuals' medical records and other protected health information. HIPAA generally applies to health plans and insurers, healthcare clearinghouses and those healthcare providers that conduct certain health care transactions electronically and sets minimum standards for Defendant's maintenance of Representative Plaintiffs' and Class Members' PHI/PII. More specifically, HIPAA requires

[4] Privacy Policy, HII, https://huntingtoningalls.com/hii-web-privacy-statement/#:~:text=HII%20does%20not%20collect%20Personal,us%20through%20our%20Online%20Activities/ (last accessed May 5, 2023).

[5] *Id.*

appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

13. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

14. Defendant claims that it "protects Personal Information under our control against—and require our service providers to also protect against—accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, Personal Information that is transmitted, stored, or otherwise processed. Only authorized employees have access to the data you provide, and that access is limited to least privileged, need to know access. HII employees who have access to your Personal Information have agreed to maintain the confidentiality of that information."[6] Representative Plaintiffs and the Class Members, some as consumers, relied on the promises and duties of HII to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

15. By obtaining, collecting, using and deriving a benefit from Representative Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiffs do not bring claims in this action for direct violations of HIPAA, but charge Defendant with various legal violations merely predicated upon the duties set forth in HIPAA.

---

[6] Privacy Policy, HII, https://huntingtoningalls.com/hii-web-privacy-statement/#:~:text=HII%20does%20not%20collect%20Personal,us%20through%20our%20Online%20Activities/ (last accessed May 5, 2023).

16. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PHI/PII was safeguarded, failing to timely notify Representative Plaintiffs and Class Members of the Breach, obfuscating the nature of the Breach, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

17. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member is a citizen of a state different from Defendant.

18. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

19. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

20. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this District, and Defendant does business in this Judicial District.

PLAINTIFFS' COMMON EXPERIENCES

21. Defendant received highly sensitive PHI/PII from Representative Plaintiffs. As a result, Representative Plaintiffs' information was among the data accessed by an unauthorized third party in the Data Breach.

22. Representative Plaintiffs were and are very careful about sharing their PHI/PII. Representative Plaintiffs have never knowingly transmitted unencrypted sensitive PHI/PII over the internet or any other unsecured source.

23. Representative Plaintiffs stored any documents containing their PHI/PII in a safe and secure location or destroyed the documents. Moreover, Representative Plaintiffs diligently chose unique usernames and passwords for their various online accounts.

24. Representative Plaintiffs took reasonable steps to maintain the confidentiality of their PHI/PII and relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

25. The Notice from Defendant notified Representative Plaintiffs that Defendant's network had been accessed and that Plaintiffs' PHI/PII may have been involved in the Data Breach.

26. Furthermore, Defendants' Notice directed Representative Plaintiffs to be vigilant and to take certain steps to protect their PHI/PII and otherwise mitigate their damages.

27. As a result of the Data Breach, Representative Plaintiffs heeded Defendant's warnings and spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice, and self-monitoring their accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured.

28. Even with a perfect response from Representative Plaintiffs, the harm caused to Representative Plaintiffs cannot be undone.

29. Representative Plaintiffs suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that Representative Plaintiffs' entrusted to Defendant, which was compromised in and as a result of the Data Breach.

30. Representative Plaintiffs suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling their PHI/PII.

31. Representative Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from their PHI/PII being placed in the hands of unauthorized third parties/criminals.

32. Representative Plaintiffs have a continuing interest in ensuring that their PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff April Darrin's Experiences

33. On or about April 13, 2023, Representative Plaintiff April Darrin was notified via letter from Defendant that her PHI and/or PII had been accessed as a result of the Data Breach.

34. Representative Plaintiff Darrin is an adult individual and, at all times relevant herein, a resident and citizen of the State of Ohio. Representative Plaintiff Darrin is a victim of the Data Breach. Defendant received Representative Plaintiff Darrin's PHI/PII in connection with her employment as a Director of Contracts with a company that was bought by Defendant. As a result, Representative Plaintiff Darrin's information was among the data accessed by an unauthorized third party in the Data Breach.

35. For about a year now, Representative Plaintiff Darrin has been receiving a combination of around 5-6 spam calls and texts (and many additional spam emails) per day. Prior to this time, she was receiving, at most, maybe one such troublesome call and/or email per day.

Representative Plaintiff Darrin is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from her to commit identity theft by way of a social engineering attack. Representative Plaintiff Darrin believes and avers that this increase in spam calls, texts and emails was a result of the Data Breach.

Plaintiff Kenneth D. Keeler's Experiences

36. On or about April 18, 2023, Representative Plaintiff Keeler was notified via letter from Defendant that his PHI and/or PII had been accessed as a result of the Data Breach.

37. Representative Plaintiff Keeler is an adult individual and, at all times relevant herein, a resident and citizen of the State of Alabama. Representative Plaintiff Keeler is a victim of the Data Breach. Defendant received Representative Plaintiff Keeler's PHI/PII in connection with the employment Representative Plaintiff Keeler had with Defendant. As a result, Representative Plaintiff Keeler's information was among the data accessed by an unauthorized third party in the Data Breach.

Plaintiff Cheryl Soles' Experiences

38. On or about April 18, 2023, Representative Plaintiff Soles was notified via letter from Defendant that her PHI and/or PII had been accessed as a result of the Data Breach.

39. Representative Plaintiff Soles is an adult individual and, at all times relevant herein, a resident and citizen of the State of Nebraska. Representative Plaintiff Soles is a victim of the Data Breach. Defendant received Representative Plaintiff Soles' PHI/PII, but, upon information and belief, Representative Plaintiff Soles is not familiar with Defendant and does not know how Defendant acquired her PHI/PII. Representative Plaintiff Soles' information was among the data accessed by an unauthorized third party in the Data Breach.

Plaintiff Tyler N. Beadle's Experiences

40. On or about April 2023, Representative Plaintiff Beadle was notified via letter from Defendant that his PHI and/or PII had been accessed as a result of the Data Breach.

41. Representative Plaintiff Beadle is an adult individual and, at all times relevant herein, a resident and citizen of the State of New Mexico. Representative Plaintiff Beadle is a victim of the Data Breach. Defendant received Representative Plaintiff Beadle's PHI/PII in

connection with Beadle's employment with a company that was purchased by Defendant. Through this work, Representative Plaintiff Beadle had top secret government clearance, which he obtained by completing Standard Form SF-86. Upon information and belief, Representative Plaintiff Beadle's Form SF-86 and/or the data contained in his Standard Form SF-86 was stolen in the Data Breach, which included the PII of his family members as well.

Plaintiff Bruce Snyder's Experiences

42. On or about April 18, 2023, Representative Plaintiff Snyder was notified via letter from Defendant that his PHI and/or PII had been accessed as a result of the Data Breach.

43. Representative Plaintiff Snyder is an adult individual and, at all times relevant herein, a resident and citizen of the State of Ohio. Representative Plaintiff Snyder is a victim of the Data Breach. Defendant received Representative Plaintiff Snyder's PHI/PII, but, upon information and belief, Representative Plaintiff Snyder is not familiar with Defendant and does not know how Defendant acquired his PHI/PII. Representative Plaintiff Snyder's information was among the data accessed by an unauthorized third party in the Data Breach.

44. In March 2023, Representative Plaintiff Snyder's information was fraudulently used to apply for a TD Retail credit card with Samsung. Representative Plaintiff Snyder did not apply for this card himself. Representative Plaintiff Snyder believes the information used to apply for this card was acquired during the Breach.

DEFENDANT

45. Defendant is a Delaware corporation with a principal place of business located at 4101 Washington Avenue, Newport News, Virginia 23607. Defendant is, primarily, a shipbuilder, producing the "majority of the U.S. Navy fleet."[7] Defendant is frequently awarded U.S. military contracts, and provides military support in multiple sectors, including cybersecurity and analytics,

[7] "*What We Do,*" https://hii.com/what-we-do/ (last accessed April 27, 2023).

and provides emergency and non-emergency medical transport services.[8] For fiscal year 2022, Defendant boasted an annual revenue of $10.67 billion.[9]

46. Defendant's services are specialized for industries and government entities that manage highly sensitive data. Thus, Defendant must oversee, manage and protect the PHI/PII of its employees, clients and third-party consumers.

47. Upon information and belief, the third-party consumers whose PHI/PII was collected by Defendant have no direct relationship with Defendant, do not want one and have never consented to its services.

48. After collecting such PHI/PII, Defendant maintains this PHI/PII in its computer systems.

49. Under state and federal law, Defendant has a duty to protect PHI/PII it collects and to notify victims of breaches of its systems.

50. In its Privacy Policy, Defendant promises that it "protect[s] Personal Information under [its] control against – and require our service providers to also protect against [] unauthorized disclosure of or access to, Personal Information that is transmitted, stored or otherwise processed." HII further declares that "consistent with [its] legal and contractual obligations and with cybersecurity best practices, [it] will use [Personal Information] to the extent necessary to maintain and improve our cybersecurity program and awareness of evolving threats [.]"[10]

51. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

---

8 *"Cyber, EW & Space,"* https://hii.com/what-we-do/capabilities/cyber-ew-space/ (last accessed April 27, 2023).

9 Huntington Ingalls Industries, Companies Market Cap, https://companiesmarketcap.com/huntington-ingalls-industries/revenue/ (last accessed July 25, 2023).

10 HII Web Privacy Statement, HII, https://huntingtoningalls.com/hii-web-privacy-statement/#:~:text=HII%20does%20not%20collect%20Personal,us%20through%20our%20Online%20Activities/ (last accessed May 5, 2023).

CLASS ACTION ALLEGATIONS

52. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiffs and the following classes/subclass(es) (collectively, the "Class(es)"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or around April 2022."
>
> **New Mexico Subclass:**
> "All individuals within the State of New Mexico whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or around April 2022."

53. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

54. In the alternative, Representative Plaintiffs request additional subclasses as necessary based on the types of PHI/PII that were compromised.

55. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

56. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the tens of

thousands of individuals. Membership in the Classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiffs and Class Members that their PHI/PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiffs' and Class Members' PHI/PII;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of each of the Plaintiff Classes in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entireties. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

57. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

58. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Classes in their entireties, not on facts or law applicable only to Representative Plaintiffs.

59. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

60. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

61. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including but not limited to full names, Social Security numbers, credit card numbers, debit card numbers, dates of birth, driver's license numbers, state identification numbers, tax identification numbers, personal identification numbers, military identification, passport numbers, financial account information, routing numbers, health insurance information and medical information. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

62. According to the Data Breach Notification, which Defendant filed with the Office of the Maine Attorney General, 43,643 persons were affected by the Data Breach.[11]

63. Representative Plaintiffs were provided the information detailed above upon Representative Plaintiffs' receipt of a letter from Defendant, dated April 18, 2023. Representative Plaintiffs were not aware of the Data Breach until receiving that letter.

Defendant's Failed Response to the Breach

64. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PHI/PII with the intent of misusing the PHI/PII, including marketing and selling Representative Plaintiffs' and Class Members' PII.

65. Not until after roughly a year after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was

[11] "*Data Breach Notification,"* https://apps.web.maine.gov/online/aeviewer/ME/40/ba2846ca-c8ca-4c24-94fa-6f239a70fbf8.shtml (last accessed April 27, 2023).

potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

66. According to the Notice, which Defendant mailed on April 18, 2023, Defendant claims to have "discovered that between March of 2022 and May of 2022, an unauthorized party who is not associated with HII engaged in an unauthorized activity involving certain file storage systems and may have accessed files that contained some of your personal information." **Exhibit A.**

67. In other words, Defendant's investigation revealed that its network had been hacked by cybercriminals for up to 91 days, and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of HII's consumers' personal and highly private PHI/PII.

68. What's worse, Representative Plaintiffs' and Class Members' PHI/PII was in the hands of cybercriminals for ***nearly a year and one month*** before they were notified of Defendant's Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

69. Despite its duties and alleged commitments to safeguard PHI/PII, HII does not follow industry standard practices in securing consumers' PHI/PII, as evidenced by the Data Breach. Upon information and belief, the PHI/PII stored on Defendant's network was not encrypted.

70. In response to the Data Breach, Defendant contends that it has or will "initiate [] measures to review and reinforce the security of its storage systems." Defendant also promises that it "will promptly take any additional steps that may be required to ensure that your personal information is protect." **Exhibit A.** Although Defendant fails to expand on what these alleged "reinforcements" and "additional steps" are, such steps and reinforcements should have been in place before the Data Breach.

71. Through its Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach and, thus, encouraged breach victims to consider credit reporting and monitoring in order to "safeguard [their] information from potential misuse." **Exhibit A.**

72. Upon information and belief, Defendant has offered a year of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PHI/PII that cannot be changed, such as Social Security numbers.

73. Defendant encouraging Representative Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgement that the impacted consumers are subject to a substantial and imminent thread of fraud and identity theft.

74. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law and its own assurances and representations to keep Representative Plaintiffs' and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

75. Representative Plaintiffs and Class Members were required to provide their PHI/PII to Defendant in order to receive services and/or employment (although some Representative Plaintiffs never sought services and/or employment with Defendant at all), and as part of providing services and/or employment, Defendant created, collected and stored Representative Plaintiffs' and Class Members' PHI/PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

76. Despite this, Representative Plaintiffs and Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiffs and Class Members are thus left to speculate as to where their PHI/PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

77. Representative Plaintiffs' and Class Members' PHI/PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Representative Plaintiffs' and/or Class Members' approval. Either way,

unauthorized individuals can now easily access Representative Plaintiffs' and Class Members' PHI/PII.

Defendant Collected/Stored Class Members' PHI/PII

78. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiffs' and Class Members' PHI/PII.

79. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PHI/PII. Defendant, in turn, stored that information on Defendant's system which was ultimately affected by the Data Breach.

80. By obtaining, collecting and storing Representative Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties over the PHI/PII and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' PHI/PII from unauthorized disclosure.

81. Representative Plaintiffs and Class Members have taken reasonable steps to maintain their PHI/PII's confidentiality. Representative Plaintiffs and Class Members relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

82. Defendant could have prevented the Data Breach, which began no later than March 2022, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' PHI/PII.

83. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

84. Due to the high-profile nature of these breaches and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing

for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

85. And yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

86. In failing to adequately secure Representative Plaintiffs' and Class Members' sensitive data, Defendant breached duties it owed Representative Plaintiffs and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to safeguard patients' PHI. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' PHI/PII. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII, independent of any statute.

87. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information") and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

88. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

89. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

90. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

91. "Electronic protected health information" is "individually identifiable health information […] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

92. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

93. HIPAA also requires Defendant to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

94. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

95. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information

is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

96. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PHI/PII.

97. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PHI/PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

98. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

99. The FTC recommends that companies not maintain information longer than is necessary for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

100. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

101. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI/PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

102. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in Defendant's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks and protocols adequately protected Representative Plaintiffs' and Class Members' PHI/PII.

103. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain and test its computer systems, servers and networks to ensure that all PHI/PII in its possession was adequately secured and protected.

104. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

105. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

106. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

107. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals'

PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust their PHI/PII to Defendant.

108. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

109. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

110. The ramifications of Defendant's failure to keep Representative Plaintiffs' and Class Members' PHI/PII secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, date of birth, Social Security number or driver's license number, without permission, to commit fraud or other crimes.

111. Moreover, while the greater efficiency of electronic health records translates to cost savings for insurance providers such as Defendant, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists, in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

112. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[14]

113. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[15] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[16] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[17]

114. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

115. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

---

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

[15] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed January 21, 2022).

[16] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed January 21, 2022).

[17] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed January 21, 2022).

116. Identity thieves can use PHI/PII, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Identity thieves can also use the stolen data to harm Representative Plaintiffs and Class Members through embarrassment, blackmail or harassment in person or online.

117. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiffs' and Class Members' PHI/PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

118. There may be a time lag between when harm occurs versus when it is discovered and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

119. At present, Defendant has offered a mere twelve months of free credit monitoring, provided by Experian, to breach victims. Clearly, Representative Plaintiffs' and Class Members' PHI/PII may exist on the dark web and in the public domain for months, or even years, before it is used for ill gains and actions. With only twelve months of monitoring, Representative Plaintiffs and Class Members remain unprotected from the real and long-term threats against their personal, sensitive and private data.

---

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

120. Moreover, data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Representative Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

121. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[19]

122. The harm to Representative Plaintiffs and Class Members is especially acute given the leaked data included medical information. Medical identity theft is one of the most common, most expensive and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[20]

123. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[21]

124. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

---

[19] Social Security Administration, https://ssa.gov/pubs/EN-05-10064.pdf/ (last accessed April 25, 2023).
[20] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed January 21, 2022).
[21] *Id*.

125. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[23]

126. And data breaches are preventable.[24] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[25] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[26]

127. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[27]

128. Here, Defendant knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were

---

22 See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed January 21, 2022).
23 Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed January 21, 2022).
24 Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
25 *Id.* at 17.
26 *Id.* at 28.
27 *Id.*

necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

129. Furthermore, Defendant has offered only a limited one-year subscription for identity theft monitoring and identity theft protection through Experian IdentityWorks. Its limitation is inadequate when the victims are likely to face many years of identity theft.

130. Moreover, Defendant's credit monitoring offer and advice to Representative Plaintiffs and Class Members squarely places the burden on Representative Plaintiffs and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Representative Plaintiffs and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Representative Plaintiffs and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions to Representative Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

131. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Representative Plaintiffs' and Class Members' PHI/PII.

132. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

COUNT ONE
Negligence
(On behalf of the Representative Plaintiffs and the Nationwide Class)

133. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

134. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' PHI/PII on its computer systems and networks.

135. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in its possession;

b. to protect Representative Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

136. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

137. Defendant knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate security, as Defendant knew about numerous, well-publicized data breaches.

138. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII.

139. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Representative Plaintiffs and Class Members had entrusted to it.

140. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII.

141. Because Defendant knew that a breach of its systems could damage tens of thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII contained thereon.

142. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

143. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

144. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party

to gather Representative Plaintiffs' and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

145. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

146. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

147. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

148. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting almost a year after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

149. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PHI/PII, and to access their medical records and histories.

150. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiffs' and Class Members' PHI/PII and the harm suffered, or risk of imminent harm suffered by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

151. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

152. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

153. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

154. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

155. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se.* Defendant also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

156. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud

and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to their healthcare, (vii) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

157. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

158. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PHI/PII in its continued possession.

COUNT TWO
Negligence *Per Se*
(On behalf of the Representative Plaintiffs and the Nationwide Class)

159. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

160. HIPAA requires that covered entities and business associates "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected

health information" and "must reasonably safeguard protected health information from any intentional or unintentional use or disclosure…." 45 CFR § 164.530(c).

161. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 requires HIPAA covered entities and their business associates to provide notification to the United States Department of Health and Human Services, prominent media outlets following a data breach or any breach of unsecured protected health information without unreasonable delay and in no event later than 60 days after discovery of a data breach.

162. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits companies such as Defendant from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect PHI/PII. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

163. In addition to the FTC rules and regulations and state law, other states and jurisdictions where victims of the Data Breach are located require that Defendant protect PHI/PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

164. Defendant violated HIPAA and FTC rules and regulations obligating companies to use reasonable measures to protect PHI/PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of a Data Breach and the exposure of Representative Plaintiffs' and Class members' highly sensitive PHI/PII.

165. Each of Defendant's statutory violations of HIPAA, Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitute negligence *per se*.

166. Representative Plaintiffs and the Class Members are within the category of persons HIPAA and the FTC Act were intended to protect.

167. The harm that occurred as a result of the Data Breach described herein is the type of harm HIPAA and the FTC Act were intended to guard against.

168. As a direct and proximate result of Defendant's negligence *per se*, Representative Plaintiffs and Class Members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PHI/PII in Defendant's possession and are entitled to damages in an amount to be proven at trial.

COUNT THREE
Breach of Implied Contract
(On behalf of the Representative Plaintiffs and the Nationwide Class)

169. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

170. Through their course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' PHI/PII.

171. Defendant required Representative Plaintiffs and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's services and/or employment with Defendant.

172. Defendant solicited and invited Representative Plaintiffs and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

173. As a condition of being consumers and/or employees of Defendant, Representative Plaintiffs and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiffs and Class Members if its data had been breached and compromised or stolen.

174. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

175. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

176. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

177. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other economic and noneconomic harm.

COUNT FOUR
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Representative Plaintiffs and the Nationwide Class)

178. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

179. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

180. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

181. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members and continued acceptance of PHI/PII and storage of other personal information after Defendant

knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

182. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FIVE
New Mexico Unfair Practices Act
N.M. Stat. Ann. §§ 57-12-2, *et seq.*
(On Behalf of Plaintiff Beadle and the New Mexico Subclass)

183. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

184. The New Mexico Plaintiff Beadle, individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the New Mexico Subclass, brings this claim.

185. Defendant is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

186. Defendant was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

187. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

188. Defendant engaged in unconscionable, unfair and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

a. Knowingly representing that its goods and services have characteristics, benefits or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5);

b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7);

c. Knowingly using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14);

d. Taking advantage of the lack of knowledge, experience or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

189. Defendant's unfair, deceptive and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New Mexico Subclass members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately improve security and privacy measures following previous industry-wide cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Mexico Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D) and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New Mexico Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Mexico Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B- 3(D) and mandating reasonable data security, N.M. Stat. § 57- 12C-4;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New Mexico Subclass Members' PHI/PII; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Mexico Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D) and mandating reasonable data security, N.M. Stat. § 57-12C-4.

190. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

191. Defendant intended to mislead Plaintiff and New Mexico Subclass Members and induce them to rely on its misrepresentations and omissions.

192. Defendant acted intentionally, knowingly and maliciously to violate New Mexico's Unfair Practices Act and recklessly disregarded Plaintiff's and New Mexico Subclass Members' rights.

193. As a direct and proximate result of Defendant's unfair, deceptive and unconscionable trade practices, Plaintiff and New Mexico Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PHI/PII.

194. Plaintiff and New Mexico Subclass Members seek all monetary and nonmonetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater) and reasonable attorneys' fees and costs.

COUNT SIX
Declaratory Judgment
(On behalf of the Representative Plaintiffs and the Nationwide Class)

195. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

196. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

197. An actual controversy has arisen in the wake of the Data Breach regarding Representative Plaintiffs' and Class Members' PHI/PII and whether Defendant is currently maintaining data security measures adequate to protect Representative Plaintiffs and Class Members from further data breaches that compromise their PHI/PII. Representative Plaintiffs

allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Representative Plaintiffs continue to suffer injury as a result of the compromise of their PHI/PII and remain at imminent risk that further compromises of their PHI/PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

198. Representative Plaintiffs and the Classes have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Representative Plaintiffs' and Class Members' PHI/PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PHI/PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Representative Plaintiffs.

199. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PHI/PII of Representative Plaintiffs and Class Members;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PHI/PII;

c. Defendant's ongoing breaches of its legal duty continue to cause Representative Plaintiffs harm.

200. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PHI/PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

201. If an injunction is not issued, Representative Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate and substantial. If another breach at Defendant occurs, Representative Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

202. The hardship to Representative Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Representative Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

203. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Representative Plaintiffs and others whose confidential information would be further compromised.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class and the New Mexico Subclasses, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify each of the proposed Classes and/or any other appropriate Subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

c. requiring Defendant to delete and purge Representative Plaintiffs' and Class Members' PHI/PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PHI/PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiff Classes and/or Subclasses, hereby demand a trial by jury for all issues triable by jury.

Dated: July 25, 2023

COLE & VAN NOTE

/s/ Scott Edward Cole
Scott Edward Cole, Esq. (CA S.B. #160744)
555 12th Street, Suite 2100
Oakland, CA 94607
Telephone: (510) 891-9800
Email: sec@colevannote.com

MASON LLP

Gary E. Mason, Esq.
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
Email: gmason@masonllp.com

TURKE & STRAUSS LLP

Raina Borrelli, Esq.
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Email: raina@turkestrauss.com

Plaintiffs' Interim Co-Lead Class Counsel

Additional Plaintiffs' Counsel

GOLOMB SPIRT GRUNFELD P.C.

Kenneth J. Grunfeld, Esq.
1835 Market Street, Suite 2900
Philadelphia, Pennsylvania 19103
Telephone: (215) 985-9177
Facsimile: (215) 985-4169
Email: KGrunfeld@GolombLegal.com

WEBSTER BOOK LLP

/s/ Steven T. Webster
Steven T. Webster, Esq. (VSB No. 31975)
300 N. Washington St., Suite 404
Alexandria, Virginia 22314
Telephone: (888) 987-9991
Email: swebster@websterbook.com

CERTIFICATE OF SERVICE

I hereby certify that, on July 25, 2023, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
Webster Book LLP